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:

A is what a cipher creates

B is correct, it is an algorithm the encrypt a message

C a cipher is not a digit

D Cipher is not code

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.

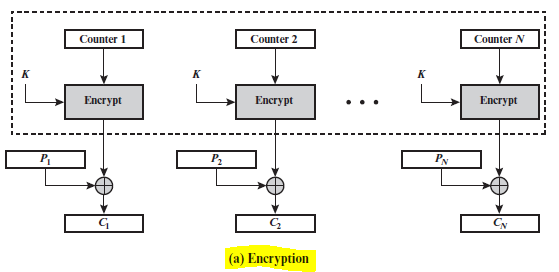
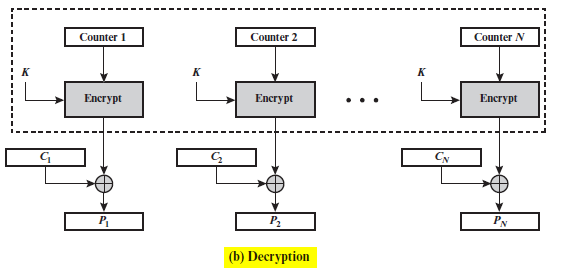
After drawing the diagram, you add the sentences that explain the mode itself

A Does it independently

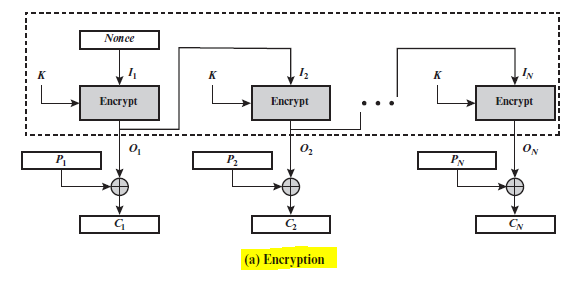
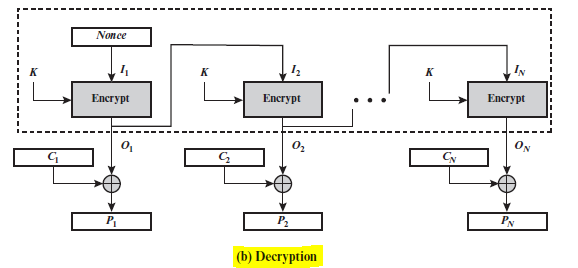
B the text gets altered every block and it is dependent on the last block

C The Key stream is XORed with the cipher text in order to generate the plaintext

D is the correct answer

**Figure.1a &1b** Counter (CTR) Mode

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

Explain Other Choices:

A Cryptography Encryption and Decryption is a method of security. These methods rely on trust.

B is the correct answer, Trust is the foundation of security in cyberspace. To achieve an organization’s security goals and objectives, organization should implement technical mechanisms to achieve high trust for its cyberspace

C Authentication is a way to establish trust We use authentication and digital signature concepts to achieve Authenticity. This is one of the added ways to ensure trust.

D Public Key Certificates – is a document issued by Certification Authority to certify the subscriber is indeed that entity.

E Digital signature is a way to authentic thus it is very similar to C

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

Explain Other Choices:

Security means the coercive capability to stop an aggressor. Security is freedom from war, and the ability to deter

or defeat aggressive attacks.

b) Security refers to safety from vulnerabilities (both external and internal) that could harm the state, societies within

the state, and the values of those societies.

c) Security means freedom to enjoy the things that are most important to human survival and well being, such as

food, health care, and the opportunity to live well.

d) D is the correct answer and these were the definition of secure and felt there was no need to explain these more.

e) None of the above.

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

Explain Other Choices:

A Counter mode is independent and run in parallel

B Cypher Block Chain Mode is depended on each block. This means we can run parallel for decryption but not for encryption.

C Electronic Codebook mode, each block is encrypted independently with the same key. This makes it easy to run in parallel.

D is the correct answer. All the above is true

E None of the above is wrong because D is correct.

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: A is correct. 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:

A a shared secret key is good and it will increase the strength of a cipher. A small key is susceptible to a brute force attack.

B Keeping the algorithm secret will not increase the strength as most algorithms are public and you want to use the once that are proven to work.

C is the correct answer Using a key with a large number of bits will protect against brute force attracts.

D is not correct because B is not true

C is not correct because A and be are true

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

Explain:

C

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

Explain:

D

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

Explain:

D

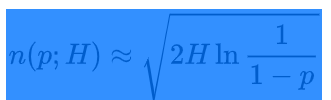
Q15: Answer (A or B or C or D or E)

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)