

Take Home Assessment I

Started: Nov 13 at 6:13pm

Quiz Instructions

Rules



- If you are uncertain about the details of a particular problem, make any reasonable assumptions that you feel are necessary to solve it.
- You are to neither give nor receive aid on this exam. The only thing you are permitted to consult while taking the exam are the lecture notes and slides.
- You may not show or discuss your exam or your solution with anyone till everyone in the class has finished taking their exam
- There is no time-limit for each attempt but students in the past had trouble when an attempt took too long or was left incomplete for a long time. Canvas sometimes lost their progress. It is best to complete each attempt in one session/sitting.

Fast Problems

Question 1

2 pts

Which of the following accurately characterizes Attack Surface? (Select one answer from below)

- ☐ Attack surface is a methodical way to explore attack paths leading to a specific attack goal
- ☒ Attack surface refers to only reachable and exploitable vulnerabilities present in an enterprise IT infrastructure
- ☐ Attack surface refers to all the vulnerabilities present in an enterprise IT infrastructure

- ☐ Attack surface refers to only exploitable vulnerabilities present in an enterprise IT infrastructure
- ☐ Attack surface refers to only physical access points to assets in an enterprise IT infrastructure

Question 2**2 pts**

A cipher that scrambles letters in the plaintext into different positions is referred to as what? (choose one)

- ☐ Stream Cipher
- ☒ Transposition Cipher
- ☐ Block Cipher
- ☐ Substitution Cipher

Question 3**2 pts**

In order to guarantee that a one time pad provides confidentiality, which of the following assumptions need to be true? (pick all that apply)

- ☐ The key is picked from a well-written well-known book
- ☐ Adversary has limited computational power
- ☒ The key used is truly random
- ☒ The key is use only once

Question 4**2 pts**

Approximate expected number of steps in an efficient brute force attack against 3DES in encrypt-decrypt-encrypt mode with three distinct keys is? (choose one)

- ☐ 2^{57}
- ☐ 2^{168}
- ☒ 2^{112}
- ☐ 2^{56}

Question 5**2 pts**

Single Sign-on helps with password re-use by reducing the number of accounts/passwords users have to maintain

- ☒ True
- ☐ False

Question 6**2 pts**

Cryptographic keys should be refreshed after a certain number of uses or after certain period of time in order to maintain security

- ☒ True
- ☐ False

Question 7**1 pts**

Alice wants to send a confidential message to Bob. To preserve confidentiality, she wants to encrypt the message using public-key cryptography. What key should she use?

- ☐ Bob's Private Key
- ☒ Bob's Public Key
- ☐ Alice's Private Key
- ☐ Alice's Public Key

Question 8**2 pts**

A bloom filter can sometimes miss detecting a bad password

- ☒ True, because a bad password's hash may sometimes index into an unset bit of the bloom filter
- ☐ True, because hashes are randomized and may index into different bits sometimes
- ☐ False, because a hash of the bad password may collide with a hash of a good password
- ☐ False, because hashes are deterministic and will always index into the same bits for the same password

Question 9**2 pts**

When an online bank sends a PIN by SMS after you have entered your account password, what factors of authentication are in play?

- ☒ Something you have
- ☒ Something you know
- ☐ Something you do
- ☐ Something you are

Question 10**2 pts**

Suppose that a server concatenates a unique 16-bit random number as salt value for every user's password and then stores the hashed password along with the salt value in a plaintext password file. How much harder does adding the salt make it for an attacker who obtains the password file to crack Alice's password?

- ☐ Not much harder at all
- ☒ About 2^{16} times, which is about 65000 times harder than it would be without the salt.
- ☐ Impossible
- ☐ About twice as hard as it would be without salt

Question 11**2 pts**

Electronic signatures can prevent messages from being:

- ☐ Disclosed
- ☐ Erased
- ☒ Repudiated
- ☐ Forwarded

Question 12**2 pts**

Alice wants to send a message to Bob. To preserve integrity, she wants to append a digital signature on her message as shown - $m \parallel \text{Sig}(m)$.

If Bob wants to verify the integrity of this message. What information would he need?

- ☐ a) Bob's Public Key and b) Alice's Public Key
- ☐ a) Bob's Private Key and b) The hash function Alice used
- ☐ a) Alice's Private Key and b) The hash function Alice used
- ☒ a) Alice's Public Key and b) The hash function Alice used

Question 13**4 pts**

Considering the initialization vectors (IVs) used in encryption modes and salts used with passwords, for each statement below select True (T) or False (F).

Salts need NOT be kept secret

True



IVs need to always be kept secret

False



IVs should not be re-used for a given key

True



Salt is meant to randomize the output of a hash on a password

True



Question 14**2 pts**

Which of the following security principle should be followed when designing a cryptographic algorithm?

- ☐ Least Privilege
- ☐ Complete Mediation
- ☐ Separation of Privilege
- ☒ Open Design

Question 15**2 pts**

Which security principle is applied when picking the size of cryptographic keys?

- ☐ Fail-close
- ☐ Detection
- ☒ Work Factor
- ☐ Keep it Simple

Not-So-Fast Problems

Use the following information to answer the next four questions:

Encryption Modes I (Parts a-d)

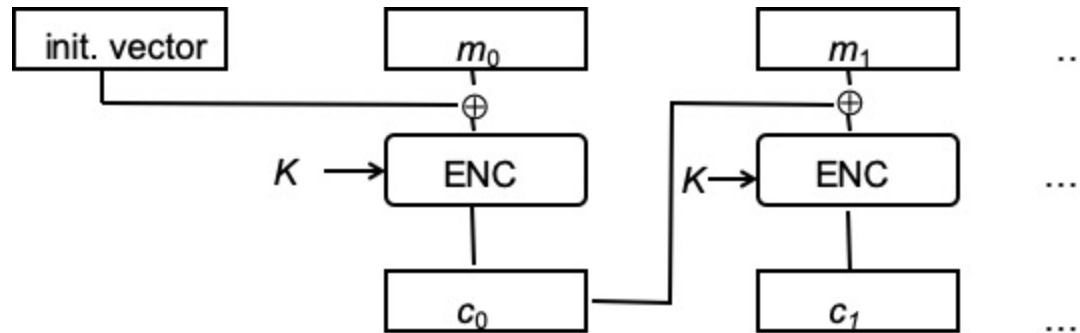


Figure above shows CBC mode for encryption. Here IV represents the initialization vector, E_k represents encryption using a block cipher with key k , and \oplus represents XOR operation respectively. CBC encryption can be described by the following equations:

$$c_0 = E_k(m_0 \oplus IV)$$

$$c_i = E_k(m_i \oplus c_{i-1}) \text{ where } i > 0$$

Question 16

4 pts

Encryption Modes I (Part b)

A message $m = m_0m_1m_2m_3m_4m_5$ is encrypted using AES with CBC mode under the key K with different initialization vectors IV_1 and $IV_2 (\neq IV_1)$ respectively. Assume that $c = c_0c_1c_2c_3c_4c_5$ is the ciphertext output when m is encrypted with key K using IV_1 , and $c' = c'_0c'_1c'_2c'_3c'_4c'_5$ is the ciphertext output when m is encrypted with key K using IV_2 . Which of the following correctly describes the relationship between c and c' . (Select one answer from below) (HINT: Use the encryption mode figure or equations shown above)

- ☐ c and c' are different but only in the first two blocks due to the self-healing property of CBC. That is, $c_i \neq c'_i$ for $i = 0, 1$ but $c_i = c'_i$ for all $i \geq 2$.
- ☒ c and c' are completely different. That is, $c_i \neq c'_i$ for all i .
- ☐ c and c' are the same and only the respective IVs transmitted with them distinguish them.
- ☐ c and c' are different but only in the first block impacted by the IVs. That is, $c_0 \neq c'_0$ but $c_i = c'_i$ for all $i \geq 1$.
- ☐ None of the above

Question 17

8 pts

Encryption Modes I (Part c)


Let us say a new encryption mode CBC'' is created by **setting** the IV in CBC mode to be a **constant** of all zeros (that is IV will always be **all zeroes** for all messages) how does this modified mode CBC'' compare with ECB in the following two scenarios?

(i) (4 pts) If a message $m = m_0m_1m_2m_3m_4m_5$ is transmitted two different times encrypted with the same key K using CBC'' mode to produce ciphertexts $c = c_0c_1c_2c_3c_4c_5$ and $c' = c'_0c'_1c'_2c'_3c'_4c'_5$ respectively, what is the relationship between c and c' and **why**? That is, will they be the same or different? And if different, which parts will be different? What would be relationship between c and c' if they are encrypted using ECB mode instead of CBC'' and why?

(ii) (4 pts) If a message $m = m_0m_1m_2m_3m_4m_5$, where $m_1 = m_3$, is encrypted with the key K using CBC'' mode to produce ciphertext $c = c_0c_1c_2c_3c_4c_5$ what is the relationship between c_1 and c_3 and **why**? That is, will they be the same or different? What would be relationship between c_1 and c_3 if the message is encrypted using ECB mode instead of CBC'' and why?

(Hint: $A \oplus B = A$ if B is all zeros).

Edit View Insert Format Tools Table

12pt Paragraph **B** *I* U A  T^2 

(i) If a message $m = m_0m_1m_2m_3m_4m_5$ is transmitted two different times encrypted with the same key K using CBC" mode to produce ciphertext $c = c_0c_1c_2c_3c_4c_5$ and $c' = c'_0c'_1c'_2c'_3c'_4c'_5$ respectively, the relationship between c and c' is completely the **same** because In CBC" mode with a constant IV of all zeros, the ciphertexts will be the same for the same input message and key. Suppose they are using ECB mode encrypted instead of CBC. In that case, the relationship between c and c' is completely the same as in ECB mode, the ciphertexts will be the same for the same input message and key because each block is independently encrypted.

(ii) In CBC mode, $IV = \text{all } 0s$, the XOR operation with the IV only occurs for the first block, if $m_1 = m_3$, then c_1 and c_3 will be the same. In ECB mode, if the input

p ▶ span



173 words



Question 18

4 pts

You are designing a password system with randomly selected passwords. The alphabet for the passwords is the set of alphanumeric characters in English -- both upper and lower case alphabet, the integers 0-9, and two special characters (@ and &). You are told that the attacker can make 4096 guesses each second. If your passwords are exactly 16 characters:

a) (2 pts) What is size of the password space (i.e., number of all possible passwords)?

b) (2 pts) How long until the attacker has a 50% probability of correctly guessing user's passwords in an offline dictionary attack? [Assume no precomputed hashes]






Edit View Insert Format Tools Table

12pt Paragraph | **B** *I* U A |  | T^2 | 

a) 26 upper cases + 26 lower cases + 10 integers + 2 special characters = 64, then there are exactly 16 characters in the password thus the number of all possible passwords is 64^{16}

b) $T = PN/G = 0.5 * 64^{16} / 4096 = 0.5 * 64^{14}$

p

  | 52 words |   

Use the following information to answer the next four questions: **Crypto Primitives and Security Properties (Parts a-e)**

Alice and Bob share two distinct symmetric keys $K1_{AB}, K2_{AB}$ with each other. They also each have a public-private key pair $(PubK_A, PriK_A)$ and $(PubK_B, PriK_B)$ respectively. Recall the notation that $x||y$ means the concatenation of x with y , $\{x\}_k$ denotes the encipherment of x using key k , $h(x)$ denotes a hash of x , and $MAC_K \{x\}$ denotes MAC of x with key K .

Question 19

4 pts

Crypto Primitives and Security Properties (Part a)

$A \rightarrow B: m || \{h(m)\}_{K1_{AB}}$

Select all of the security properties/guarantees that the above transmission provides to Bob (B) from the following list:

- message integrity
- origin authenticity
- confidentiality
- None

☐ Confidentiality

☐ None

☒ Message integrity

☐ Origin authenticity

Question 20

2 pts

Justify the answers (security properties) you selected above.

Edit View Insert Format Tools Table

12pt ▾ Paragraph ▾ | **B** *I* U A ▾  ▾ τ^2 ▾ | ⋮

Message integrity: Let's assume $m = \text{"hello"}$, so Alice sends $\text{"hello"} + \{h(\text{"hello"})\}_{k1AB}$, so even if there is someone who changed the message "hello" during the transmission, Bob still can tell if the message was altered or tampered because the hash function. In addition, the attacker does not have the ability to change the corresponding concatenated message because they do not have access to the symmetric key.

p



69 words

**Question 21****4 pts****Crypto Primitives and Security Properties (Part b)**

$$A \rightarrow B: \{m\}_{K1_{AB}} || \{m\}_{K2_{AB}}$$

Select all of the security properties/guarantees that the above transmission provides to Bob (B) from the following list:

- message integrity
- origin authenticity
- confidentiality
- None

☒ Confidentiality

☐ Origin Authenticity

☒ Message Integrity

☐ None
Question 22**2 pts**

Justify the answers (security properties) you selected above.

Edit View Insert Format Tools Table

12pt Paragraph **B** *I* U A τ^2

Confidentiality: The message m is encrypted twice, this double encryption provides a level of confidentiality.

Message Integrity: Because the same message is encrypted twice with distinct

shared symmetric keys if an attacker changes the first part, they will not know how to change the corresponding second part.

p



47 words

**Question 23****4 pts****Crypto Primitives and Security Properties (Part c)**

$$A \rightarrow B: \{h(m)\}_{K1_{AB}}$$

Select all of the security properties/guarantees that the above transmission provides to Bob (B) from the following list:

- message integrity
- origin authenticity
- confidentiality
- None

☐ Origin authenticity☒ Confidentiality☐ None☐ Message integrity**Question 24****2 pts**

Justify the answers (security properties) you selected above.

Edit View Insert Format Tools Table

12pt ▾ Paragraph ▾ | **B** *I* U A ▾  ▾ T^2 ▾ | ⋮

Confidentiality: Because the output of the hash function is encrypted, the message is confidential. But the problem is that the receiver is not able to use the output of the hash function to compare it to anything, therefore the receiver is not able to determine if the message was changed in transit (message integrity), or if the message actually came from the correct person (no digital signature)

p



67 words



Question 25

4 pts

Crypto Primitives and Security Properties (Part d)

$A \rightarrow B: \{m || h(m)\}_{K1_{AB}}$

Select all of the security properties/guarantees that the above transmission provides to Bob (B) from the following list:

- message integrity
- origin authenticity
- confidentiality
- None


☒ Confidentiality

- ☐ None
- ☐ Origin authenticity
- ☒ Message integrity

Question 26**2 pts**

Justify the answers (security properties) you selected above.

Edit View Insert Format Tools Table

12pt ▾ Paragraph ▾ | **B** *I* U A ▾  ▾ τ^2 ▾ | ⋮

Confidentiality: It is encrypted with symmetric key k_{1AB} , the encryption provides confidentiality.

Message integrity: because the hash function is included along with the message m , and the entire concatenated value is encrypted with K_{AB} . this allows Bob(b) to verify the integrity of the message.

p



45 words

</>

**Question 27****4 pts****Crypto Primitives and Security Properties (Part e)**

$$A \rightarrow B: \{m\}_{PubK_A} || \{h(m)\}_{PriK_A}$$

Select all of the security properties/guarantees that the above transmission provides to Bob (B) from the following list:

- message integrity
- origin authenticity
- confidentiality
- None

☒ None

☐ message integrity

☐ origin integrity

☐ confidentiality

Question 28

2 pts

Justify the answers (security properties) you selected above.

Edit View Insert Format Tools Table

12pt ▾ Paragraph ▾ | **B** *I* U A ▾  ▾ T^2 ▾ | ⋮

None: The reason none is that Alice encrypted the message with her own public key which causes Bob to be unable to decrypt the message because he doesn't have access to Alice's private key. Even though there is a digital signature, there is nothing to compare it to in order to verify the legitimate sender. Likewise, if the message is changed and in transit, there is nothing to compare and verify the integrity.

p

  | 73 words |   ⋮

Question 29

8 pts

One-Time Password Protocols

Consider a toy hash function $h(i) = (i + 5) \bmod 13$. Suppose it is used in an implementation of the S/Key protocol. Let the initial seed value be 7. Answer the following questions

- (4 pts) Compute and show the full S/KEY hash chain.
- (2 pts) What would be the value that the server will need to store to help authenticate the user for the **first** time?
- (2 pts) What would be the password that the user needs to supply for the **fifth** login?

Edit View Insert Format Tools Table

12pt Paragraph | **B** *I* U A | | T^2 |

| | | | |

- K7: $h(11) = (11 + 5) \bmod 13 = 3$

- K8: $h(3) = (3 + 5) \bmod 13 = 8$

- K9: $h(8) = 0$

- K10: $h(0) = 5$

- K11: $h(5) = 10$

- K12: $h(10) = 2$

- K13: $h(2) = 7$

- K14: $h(7) = 12$

b. The K_{n+1} will be stored which means K15 : $h(12) = (12 + 5) \bmod 13 = 4$

c. The password is stored in a reversed order: the 5th login is 5

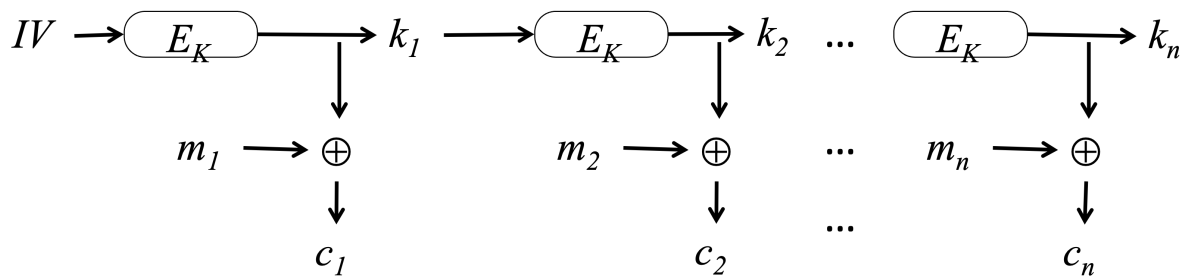
p

¹ | 135 words |

Question 30

0 pts

BONUS (5 pts)



- (1 pts) What is the encryption mode shown above?
- (2 pts) Is the above mode secure when used with public-key encryption scheme like RSA, i.e., E_K is instantiated with RSA encryption, when ciphertext $c = c_1 c_2 c_3 \dots c_n$ and $k_{n+1} = E_K(k_n)$ are transmitted to the receiver. (IV is not transmitted)?
- (2 pts) Justify your answer for part (b) above.

Edit View Insert Format Tools Table

12pt Paragraph **B** *I* U A \top^2 a. **OFB(output feedback mode)**b, **not secure**

c. Because In OFB mode, a block cipher is used to generate a keystream, which is then XORed with the plaintext to produce the ciphertext. The keystream generation in OFB mode depends on an Initialization Vector (IV) and an internal state (usually the previous ciphertext block) to produce the next keystream block. In a typical use case, the IV is transmitted along with the ciphertext to allow the receiver to regenerate the same keystream. Using RSA for encryption does not align with the principles of OFB mode. RSA encryption operates differently, using public keys to encrypt data, and it doesn't involve generating a keystream in the same way OFB does.

p

² | 114 words |

Quiz saved at 12:23am

Submit Quiz