Take Home Assessment I

Started: Nov 10 at 1:48pm

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

- (●) Attack surface refers to all the vulnerabilities present in an enterprise IT infrastructure
- ( ) Attack surface is a methodical way to explore attack paths leading to a specific attack goal

Question 2

2 pts

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

- ( ) Block Cipher
- (●) Transposition Cipher
- ( ) Stream 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)

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

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^{56}
- ○ 2^{168}
- ◉ 2^{112}
- ○ 2^{57}

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?

- ○ Alice's Public Key
- ◉ Bob's Public Key
- ○ Alice's Private Key
- ○ Bob's Private Key

Question 8

2 pts

A bloom filter can sometimes miss detecting a bad password

- ○ False, because hashes are deterministic and will always index into the same bits for the same password
- ○ True, because hashes are randomized and may index into different bits sometimes
- ◉ True, because a bad password's hash may sometimes index into an unset bit of the bloom filter
- ○ False, because a hash of the bad password may collide with a hash of a good 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 are
- [x] Something you have
- [ ] Something you do
- [x] Something you know

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?

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

Question 11

2 pts

Electronic signatures can prevent messages from being:

- ( ) Erased
- ( ) Disclosed
- ( ) Forwarded
- (●) Repudiated

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 - $m \parallel Sig(m)$.

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 Public Key and b) The hash function Alice used
- ○ a) Alice's Private 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?

- ○ Complete Mediation
- ○ Separation of Privilege
- ○ Least Privilege
- ◉ Open Design

Question 15

2 pts

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

- ○ Detection
- ○ Fail-close
- ◉ 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)

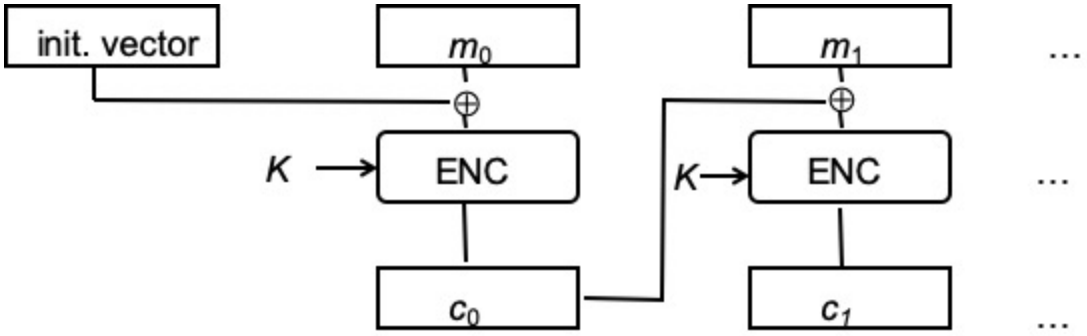


Figure above shows CBC mode for encryption. Here *IV* represents the initialization vector, E_k represents encryption using a block cipher with key *k*, and ⊕ represents *XOR* operation respectively. CBC encryption can be described by the following equations:

$c_0 = E_k(m_0 \oplus IV)$

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

Question 16

4 pts

Encryption Modes I (Part b)

A message $m = m_0 m_1 m_2 m_3 m_4 m_5$ 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 $c = c_0 c_1 c_2 c_3 c_4 c_5$ is the ciphertext output when m is encrypted with key ***K*** using IV_1, and $c' = c'_0 c'_1 c'_2 c'_3 c'_4 c'_5$ 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 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
- ○ c and c' are the same and only the respective IVs transmitted with them distinguish them.
- ◉ c and c' are completely different. That is, $c_i \neq c'_i$ for all i.

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 $m = m_0 m_1 m_2 m_3 m_4 m_5$ is transmitted two different times encrypted with the same key ***K*** using *CBC"* mode to produce ciphertexts $c = c_0 c_1 c_2 c_3 c_4 c_5$ and $c' = c'_0 c'_1 c'_2 c'_3 c'_4 c'_5$ 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 $m = m_0 m_1 m_2 m_3 m_4 m_5$, where $m_1 = m_3$, is encrypted with the key ***K*** using *CBC"* mode to produce ciphertext $c = c_0 c_1 c_2 c_3 c_4 c_5$ 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

If you transmit the same message m twice, encrypted with the same key K using CBC mode, you will get two different ciphertext c and c', This is because CBC mode introduces dependencies between the blocks, and the all-zero IV will be XORed with the first plaintext block in both case, producing different values for c0 and c'0. the C and C' will be completely different, in other words, the differences will occur in all blocks (c0, c1, c2, c3, c4, c5). If you were to encrypt the same message using ECB mode instead of CBC'', the result would be the same ciphertext for the same plaintext message. This is because ECB mode encrypts each block independently and does not introduce any dependencies or use an IV. Therefore, the output of the encryption for each block is solely dependent on the block and the key. So, c and c' would be the same if encrypted using ECB mode.

p ▸ span 159 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

characters + 10(0-9 digits) = 64 characters and there are 16 characters in my password.

2) Estimate the point at which there's a 50% chance of a successful guess:
√(64^16) ≈ 64^8≈1.8446744×10^19

Since the attacker can make 4096 guesses per second:
(1.8446744×10^19 guesses) / (4096 guesses/second) ≈ 4.50658302×1015 seconds

Thus the attacker needs 1.1541 × 10^11 seconds has a 30% probability of correctly guessing user's passwords in an offline dictionary attack.

p 2 120 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

- [x] Message integrity
- [ ] Confidentiality
- [ ] None
- [ ] 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 T²

message integrity : because it includes a hash of the message `m` encrypted with the shared key `k1AB`. Bob can verify the integrity of the message by decrypting the hash and comparing it to the hash of the message he received. If the two hashes are the same, then Bob can be confident that the message has not been tampered with in transit.

p 62 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

- [x] Confidentiality
- [ ] None
- [x] Origin Authenticity
- [ ] Message Integrity

Question 22 2 pts

Justify the answers (security properties) you selected above.

Edit View Insert Format Tools Table

12pt Paragraph B I U A T²

Confidentiality: The message m is encrypted with the shared key K1AB, so only Bob, who has the shared key, can decrypt it. An attacker who intercepts the message will not be able to read it.

Origin authenticity: The message m is also encrypted with the shared key k2AB. Since Bob is the only one who knows k2AB, he can be sure that the message came from Alice. An attacker cannot create a new message m', encrypt it with k2AB, and send it to Bob, because the attacker does not know k2AB.

p ▸ span 91 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

- [x] Message integrity
- [ ] None
- [x] Confidentiality
- [ ] Origin authenticity

Question 24

2 pts

Justify the answers (security properties) you selected above.

Edit View Insert Format Tools Table

12pt Paragraph

Message integrity: hash function provides integrity

Confidentiality: encryption provides the confidentiality.

p 11 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

- [x] Message integrity

- [ ] None
- [x] Confidentiality
- [ ] Origin authenticity

Question 26

2 pts

Justify the answers (security properties) you selected above.

Edit View Insert Format Tools Table

12pt Paragraph

Confidentiality: the usage of symmetric key.

Message integrity: it provided by the hash function {(m||h(m)} K1AB

p 20 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

- [ ] confidentiality
- [x] None
- [ ] origin integrity
- [ ] message integrity

Question 28

2 pts

Justify the answers (security properties) you selected above.

Edit View Insert Format Tools Table

12pt Paragraph B I U A T²

The answer is none, because Alice encrypted the message with the Public key which causes BOB cant read his message, thus, there is none.

p 24 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

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

Edit View Insert Format Tools Table

12px Paragraph

a. h(7) = (7+5)mod 13 = 12, h(12) = (12+5)%13 = 4, h(4) = (4+5)mod 13 = 9, h(9) = (9+5)mod 13 = 1, h(1) = (1+5)mod 13 = 6

b. It only needs to save k_n+1: here is $K_{8 = 8}$

C, User needs to supply 6 as the 5th login

p ▸ sup ▸ span ▸ span

1

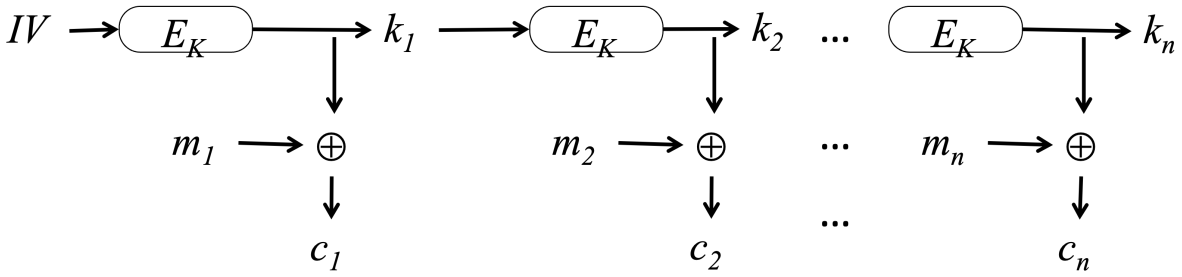
64 words

</>

Question 30

0 pts

BONUS (5 pts)



a. (1 pts) What is the encryption mode shown above?

b. (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 $c = c_1 c_2 c_3 \ldots c_n$ and $k_{n+1} = E_K(k_n)$ are transmitted to the receiver. (***IV*** is not transmitted)?

c. (2 pts) Justify your answer for part (b) above.

Edit View Insert Format Tools Table

12pt Paragraph B I U A T²

a. The shown above is OFB (output feedback mode)

b. Its not secure when use public-key encryption shceme like RSA.

c. The reason is not secure is 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 136 words </>

Quiz saved at 3:34pm

Submit Quiz