CS458-01/02/03 - Fall 2018
Practice Problem Set 2
No submission is needed

Problem 1: Circle (one) the right answer

1.1. Digital signatures can prevent messages from being:

(a) Erased
(b) Forwarded
(c) Disclosed
(d) Repudiated

1.2. What is the justification for using a message digest in digital signatures?

(a) To indicate the encryption algorithm
(b) To confirm the identity of the sender
(c) To enable transmission in a digital format
(d) To detect any alteration of the message

1.3. Suppose that a server concatenates a unique `12`-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.

(i) How much harder does adding the salt make it for an attacker who obtains the password file to crack Alice's password?
   (a) Not much harder at all
   (b) About twice as hard as it would be without salt
   (c) About 2^{12}, which is `4096` times harder than it would be without the salt.
   (d) Impossible

(ii) How much harder does the addition of salt make it for an attacker who wants to carry out offline dictionary attacks on all user passwords?
   (a) Not much harder at all
   (b) About twice as hard as it would be without salt
   (c) About 2^{12}, which is `4096` times harder than it would be without the salt.
   (d) Impossible

1.4. Suppose, Alice used `CBC` mode to encrypt her file. However, she forgot the Initializing Vector (IV) she used. If she has the ciphertext and the key, can she still decrypt the file?

(a) No, she cannot recover anything.
(b) She can recover everything except the very first block
(c) She can recover everything except the very first block and second block
(d) She can recover only the very last block

1.5. In order to know that a one-time pad provides confidentiality, which of these do we need to assume about the adversary?

(a) Has limited computational power
(b) Does not know anything about the key
(c) Attacker cannot modify the message

(d) Attacker can intercept the message

1.6. Suppose Alice has $K_{pr,A}$ as private key and $K_{pub,A}$ as public key. Bob has $K_{pr,B}$ as private key and $K_{pub,B}$ as public key. Which of the following messages will allow Alice to send m so Bob is ensured that it was generated by Alice and no one has breached its confidentiality. Here $E_{K_X}(m)$ denotes enciphering of m by the key K_X and || denotes concatenation.

(a) $E_{K_{pr,A}}(m)||E_{K_{pub,B}}(m)$

(b) $E_{K_{pr,B}}(m)||E_{K_{pub,A}}(m)$

(c) $E_{K_{pub,B}}(E_{K_{pr,A}}(m))$

(d) $E_{K_{pr,A}}(E_{K_{pub,B}}(m))$

1.7. Suppose you are working as the security administrator at *xyz.com*. You set permissions on a file object in a network operating system, which uses **DAC** (Discretionary Access Control). The **ACL** (Access Control List) of the file is as follows:

	Read	*Write*	*Execute*
Owner	×	×	×
User A	×	×	–
User B	–	–	–
Sales	×	–	–
Marketing	–	×	–
Other	×	×	–

User A is the owner of the file. User B is a member of the Sales group. What effective permissions does User B have on the file?

(a) User B has no permissions on the file.

(b) User B has *Read* permissions on the file.

(c) User B has *read* and *Write* permissions on the file.

(d) User B has *read, write* and *execute* permissions on the file.

1.8. Consider a Role-Based Access Control (RBAC) system where a role **R1** and role **R2** are mutually exclusive roles. **R1** has permissions to perform operations Review and Approve on resource Report, and **R2** has permissions to perform operation Edit on resource Report. No other role in the system has permissions to perform any operation on resource Report. Which of the following statements CANNOT be true in this setting?

(a) A Users Alice and Bob can both be assigned to **R1**.

(b) User Alice can be assigned to **R1** and user Bob can be assigned to **R2**.

(c) User Candice can Edit resource Report and Review her edits to Report.

(d) Users Eve and Mallory can both be assigned to **R2**.

1.9. Which of the following statements is NOT true about Role-Based Access Control (RBAC)?

(a) A user can be assigned one or more roles

(b) A session can have one or more users

(c) A session can have one or more roles

(d) A role can be assigned to one or more users

Problem 2

Consider the following three kinds of attack on a cryptosystem: cipher-text only, known plaintext, chosen plaintext. For each type of attacks list the information that needs to be available to an attacker.

Problem 3

In access control, what does an `open policy` mean? What does a `closed policy`' mean? What is the principle of tranquility? Which principle supports least privilege better, strong tranquility or weak tranquility?

Problem 4

Consider a computer system with three users: Alice, Bob, and Donna. Alice owns the file `AlReport`, and Bob and Donna can read it. Donna can read and write Bob's file `BOReport`, but Alice can only read it. Only Donna can read and write her file `DOReport`. Assume that the owner of each of these files can execute it.

(a) Create the corresponding access control matrix.

- if a user has read/write/execution permission on a file, write as **rwx**
- if a user has read/write permission on a file, write as **rw-**
- if a user has read permission only on a file, write as **r - -**
- if a user has no permission on a file, write as **- - -**

	AlReport	*BOReport*	*DOReport*
Alice			
Bob			
Donna			

(b) Donna gives Alice permission to read `DOReport`, and Alice removes Bob's ability to read `ALReport`. Show the new access control matrix.

	AlReport	*BOReport*	*DOReport*
Alice			
Bob			
Donna			

Problem 5

A role **R1** has read permissions to objects classified at `Secret` and `Top Secret` levels. **R1** also has append (write-only) permissions to objects classified at `Restricted` and `Secret` levels. A role **R2** has read permissions to objects classified at `Restricted` and `Secret` levels. **R2** also has append (write-only) permissions to objects classified at `Secret` and `Top-Secret` levels.

(Assume `Unrestricted` $<$ `Restricted` $<$ `Secret` $<$ `Top Secret`, and that `Bell-LaPadula model` is in use.)

(a) What is the read-level of role **R1**?

(b) What is the write-level of role **R1**?

(c) Alice has clearance level of `Secret`. Can Alice be assigned to Role **R2** - why or why not?

(d) If we want to assign Bob to Role **R1** what clearance level should he be given? Explain.

Problem 6

Given some subjects and objects in a `BLP-modeled MAC system`. Bigger number means higher clearance (5 = top secret, 1 = unclassified).

Subject	*Clearance*
Alice	3
Bob	2
Charlie	5
Dave	1

Object	*Clearance*
X	4
Y	5
Z	3
W	1

Fill in the access rights each subject has on each object (read, write, read+write, or no access). Remember `write` doesn't imply `read` in BLP model.

	X	*Y*	*Z*	*W*
Alice				
Bob				
Charlie				
Dave				