ECE 750: Usable Security and Privacy - Final	Marks obtained ↓
Date: Aug 8, 2024, Total questions: **4** Total points: **50**	
ID: Name:	Time: 2.5 hrs

Page:	2	3	4	5	6	7	9	Total
Points:	8	6	10	10	6	5	5	50
Score:								

Instructions

No aids allowed. All you are allowed is a pen and pencil.

Use space provided. Answer the questions in the spaces provided. If you run out of room for an answer you can use the back of the page but clearly note in the original answer space that the back was used.

Point value in right-hand margin. The number of points each question is worth is listed in the right hand margin. The number of points and the space provided are roughly indicative of how long of an answer is expected.

Pencils and pens allowed. Both pens and pencils are allowed. Pencil marks need to be clearly present or erased. If it is unclear if a mark is or is not present then it is up to the discretion of the grader and this point cannot be contested later.

Scratch paper. At the end of the exam there are two blank pages marked “SCRATCH PAPER”, you may tear these off and use them as scratch paper.

Passwords

1. Imagine an attacker was able to gain access to the shadow password file on a Linux server. The file contains usernames, hashed passwords, and their associated salts. The attacker wants to find the passwords of users like root.

   (a) We learned about online and offline password guessing attacks. Is the attacker most likely to use an online or an offline attack in the above situation? Briefly describe what about the situation makes your chosen attack the most appropriate for the attacker. (4)

   (b) Imagine a user is assigned a 4 character password randomly selected from a possible set of 56 characters. The password is used on a website that uses lockout. If more than 10 passwords are attempted against 1 user name, then the system locks the account for 24 hours. Under what assumptions might this password be considered sufficiently secure? (4)

2. Long random passwords are better for security because they are harder to guess. But long truly random passwords are bad for usability because they are challenging for people to remember.

   To better understand what length random password people can reliably remember Edith designs an online user study. She recruits people using an online survey platform like Amazon Mechanical Turk and requires them to have a high positive rating on the platform. She uses survey software to create an online experiment where users see information and answer questions via a webpage. Users in her study go through the following steps:

   1. Consents to be part of research.
   2. Software randomly decides if they will get a 6, 9 or 12 character password, and then creates and records a random password of that length containing at least one upper case, one lower case, one number, and one symbol. The user is shown the password and told they will need to enter this password later in the study.
   3. On the next page the user is asked to enter the password to make sure they remember it, if they enter the wrong password, they are shown the password again and reminded they need to remember it.
   4. The user then fills out the IUIPC scale.
   5. The user is asked to enter their password. No feedback is given about if it is correct or wrong.
   6. The user then fills out the SeBIS scale.
   7. The user is asked to enter their password. No feedback is given about if it is correct or wrong.
   8. The user fills out a set of demographics questions including age, gender, native language, and current ocupation.
   9. The user is asked to enter their password. No feedback is given about if it is correct or wrong.
   10. They are thanked for taking part in the survey.

   To analyze the results, Edith counts how many times participants enter their password correctly on steps 5, 7, and 9 producing a score between 0 and 3. She then uses t-tests to see if there is a statistically significantly difference in the mean number of errors between each pair of password lengths.

   Answer the questions below about the study. Feel free to use the step numbers above in your answers.

   (a) List the **independent** variable(s) Edith is collecting in her study. (3)

   (b) List the **dependent** variable(s) Edith is collecting in her study. (3)

(c) The study has several internal validity problems. Describe one of them. (6)

(d) Like all studies, this study has some external validity limitations. Describe one external validity limitation. (4)

Public/Private Key Cryptography

3. (a) Fill in the blanks in the following text describing Alice and Bob correctly communicating securely. Each blank needs to be filled in using one of the following words: (6)

- Encrypt, encrypted, encrypts
- Decrypt, decrypted, decrypts
- Sign, signed, signs, signature
- Public
- Private

Alice wants to send an encrypted and signed message to Bob who she has met in the past. When they last met in person they verified and then ***signed*** each other's __________ keys using their respective __________ keys.

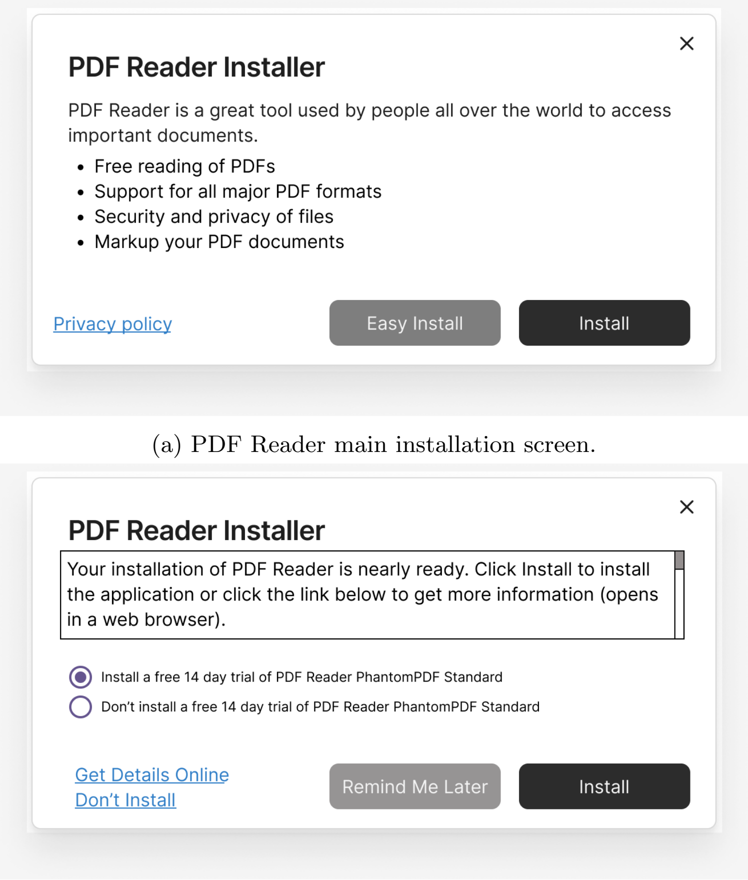
To send an email to Bob, Alice first ***signed*** the message using her __________ key and then __________ the resulting message using Bob's __________ key. Alice then sends the message over an untrusted connection.

Bob receives the message and first __________ it using his __________ key. He then verifies that the message really was from Alice by verifying the ***signed*** using Alice's __________ key.

(b) Research, such as the *Why Johnny Can't Encrypt* paper, often mentions "confusing metaphores" in regards to encryption interfaces. Give a specific example of a metaphor related to encryption that is likely confusing for people. (4)

(c) Would Alice and Bob's security in the interaction above be improved by using a Certificate Authority (CA)? State 'Yes' or 'No' and then briefly explain what a CA would do to help Alice and Bob OR explain why their current security practices are equal to or better than what a CA would provide. (6)

Design Layout



PDF Reader Installer

PDF Reader is a great tool used by people all over the world to access important documents.

- Free reading of PDFs
- Support for all major PDF formats
- Security and privacy of files
- Markup your PDF documents

(a) PDF Reader main installation screen.

PDF Reader Installer

Your installation of PDF Reader is nearly ready. Click Install to install the application or click the link below to get more information (opens in a web browser).

● Install a free 14 day trial of PDF Reader PhantomPDF Standard

○ Don't install a free 14 day trial of PDF Reader PhantomPDF Standard

(b) Installation screen for PDF Reader addon PhantomPDF Standard.

Figure 1: Two screens the user encounters when trying to install PDF Reader.

4. Figure 1b is an example of deceptive design. The user is trying to install an application called "PDF Reader". The first screen they see is the main installation screen (a). They click 'Install' and screen (b) appears. Screen (b) is offering to install a free trial of "PDF Reader PhantomPDF Standard" in addition to the "PDF Reader" software the user is trying to install. Clicking "Install" on screen (b) will install both PDF Reader Installer *and* PDF Reader PhandomPDF Standard. Clicking "Don't Install" on screen (b) will install only PDF Reader Installer which is what the user wants to install.

   (a) Use the Gestalt Principles on visual grouping to explain why a user might have trouble realizing that the "Don't Install" option in Figure 1b is a button similar to "Install" rather than a web link similar to "Get Details Online". (5)

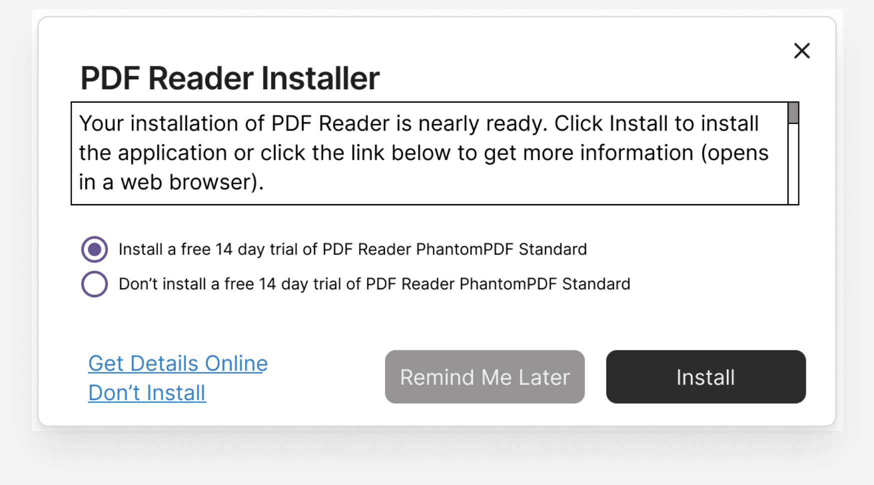
   Gestalt Principles: 1. Proximity 2. Similarity 3. Continuity 4. Closure 5. Symmetry 6. Figure/Ground 7. Common Fate

QUESTION 4 ANSWER SPACE

(b) Draw an improved sketch of Figure 1b. The design does not need to be super detailed, but all the buttons need to be clearly labeled and it should be clear where text from the original design was moved or adjusted. (5)

A copy of Figure 1b also appears on the scratch paper at the end of the exam.

SCRATCH PAPER - ok to tear off



PDF Reader Installer

Your installation of PDF Reader is nearly ready. Click Install to install the application or click the link below to get more information (opens in a web browser).

● Install a free 14 day trial of PDF Reader PhantomPDF Standard

○ Don’t install a free 14 day trial of PDF Reader PhantomPDF Standard

Figure 2: Copy of Figure 1b

SCRATCH PAPER - ok to tear off