INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

End-Autumn Semester Examination 2022-23

Date of Examination: _23rd November, 2022 ________________ Session: (FN/AN) _FN

______________________________ Duration: 3 hrs. Full Marks: __80 _

Subject No.: __CS60081__________ ______________________

Subject: _________Usable Security and Privacy______________ ______________________

Department/Center/School: ______Department of Computer Science and Engineering________

Specific charts, graph paper, log book etc., required ______________________

Special Instructions (if any): ____N/A______________________

Question 1 | 4 + 5 + 2 = 11 marks

This question is based on the definition of Cohen's kappa metric. Please show the calculation / explain your answers for each question (stating only answers will not be awarded marks).

1.1. Imagine during coding two coders C_1 and C_2 are assigning any one of the three labels L_1, L_2 and L_3 to each piece of text. Ultimately, they arrived at the following confusion matric at the end of one round of coding:

		Coder C_2		
Coder C_1		**L_1**	**L_2**	**L_3**
	L_1	120n	50n	100n
	L_2	5n	100n	30n
	L_3	25n	10n	50n

Now, consider the labels L_2 and L_3 are merged (used as one code) after discussion, compute he inter-rater agreement (Cohen's kappa value) in the table above.

1.2. Now Imagine during coding two coders C_1 and C_2 are assigning any one of the k labels L_1, L_2, L_3 ... L_k to each piece of text. Ultimately, they arrived at the following confusion matrix after one round of coding:

		Coder C2				
Coder C1		**L_1**	**L_2**		**L_{k-1}**	**L_k**
	L_1	kn	(k-1) n	...	2n	n
	L_2	n	kn	.	3n	2n
	L_3	2n	n	.	4n	3n
	...	...	...	.	...	...
	L_{k-1}	(k-2)n	(k-3)n	.	kn	(k-1)n
	L_k	(k-1)n	(k-2)n	.	n	kn

Compute the Cohen's kappa for this table and show that in this labelling for all k > 1 and n>1, 0 < Cohen's kappa < $\frac{1}{k}$

1.4. From the Cohen's kappa value found above identify one problem with the coding process? How do you systematically resolve the problem?

Question 2 | 8 x 1.5 = 12 marks

- You have now completed the Usable Privacy and Security course and Arun, a friend of yours approached you for your help. He wants to run a study to know the usability of his new UPI payment app---truePay. truePay is based on the idea of the truecaller app. When you attempt to send money to a user, truePay checks their database and notify you if the recipient account is involved in any reported scam or not. Now, of course Arun needs to know if his app truePay is as usable compared to available apps like GPay. So, he (with your help of course) designed a survey to uncover it. Since, he will be paying each participant, he wants to figure out the analysis plan first. Arun created a *between-subjects* design with a group of Campus residents who are current users of Gpay, an existing app.

  - **1.1.** What is one *measurable* dependent variable in Arun's experiment?
  - **1.2.** Write a suitable H_0 for Arun's experiment
  - **1.3.** What statistical test would you suggest for Arun's experiment for checking the hypothesis? Why? (no marks without explanation)
  - **1.4.** What is the interpretation of Type-II error in Arun's design?
  - **1.5.** What is the interpretation of effect size in Arun's design?

- Arun now wants to check what is his target population? In other words which demographics he can nudge to adapt truePay. For this purpose, he created a full factorial design for truePay and created another survey. In this survey he plans to collect answer to the question: "*Are you willing to continue using* truePay on a daily basis" with 5-point Likert scale options. He will also collect demographics of his participants: age, gender, educational qualification, average daily amount of UPI transaction (in inr) and average daily frequency of using UPI apps (in inr).

  - **1.6.** What is/are the statistical test(s) Arun should use on the survey data for finding his target population? Why? (no marks without explanation)
  - **1.7.** How will he use the proposed test to find answer to his question? Write the procedure (in 2—4 sentences)
  - **1.8.** How would Arun systematically decide what is the number of participants needed

Question 3 | (3 x 2) + 1 + 3 = 10 marks

Arun is feeling inspired and now decides to run a qualitative interview study to understand *why* people living in IIT Kharagpur use security and privacy tools for sending encrypted chat. He decided to record the interviews of his participants and then transcribe the data into text for analysis. Answer the following questions.

3.1. Which coding technique might Arun use to answer each of the question below? Why? (Just naming the technique will not be awarded any marks)

A) How many participants are currently using encrypted chat messenger knowingly?
B) Which encrypted chat messenger those participants are using?
C) Why are they using encrypted chat messenger?

3.2. Why would it be important for Arun to have a second person also participate in the process described in question above? Give one clear reason.

3.3. How should Arun integrate this second person into the process to get final codes?

3.4. Arun was told to prepare an IRB submission. What purpose does the IRB serve in human-subjects research?

Question 4 | (4 x 2) = 8 marks

Arun has now sold his truePay startup to Gpay (obviously) and recruited by the city of Kharagpur to look over their IT department. He still needs your help with his job. Arun creates a new domain, `www.khragpurcity.io` and want to set up HTTPS for better security

4.1. Arun heard that he needs to get a HTTPS certificate and for that he needs to approach a Certificate Authority (CA). Describe what the certificate will do (one sentence).

4.2. Arun wants to eliminate the step of approaching the CA and ask you to create a *self-signed* certificate for his domain. Would he face any problem(s) with such a certificate? Why or why not?

4.3. Arun is now very careful and only visits websites over HTTPS while at work. Is his employer (the City of Kharagpur) still able to tell which exact urls does he visit? Why or why not? (no marks without explanation)

4.4. Hackers from *Institute of Infinite Tranquility* are attempting to guess the Kharagpur-mayor's password. They attempt to log in over and over with likely passwords. What are two possible steps Arun can take to minimize the chance of them succeeding (without contacting the Mayor of course, they are currently on vacation)?

Question 5 | 2 + 4 + 6 + 7 = 19 marks

Imagine that you are given a password of 32 NeuKlingon language symbols (i.e., NeuKlingon alphabet). NeuKlingon alphabet contains 16 symbols. Moreover, the password is a concatenation of 4 words, each word comprising of 8 symbols. These 4 words are chosen at random (*with repetition*) from a word dictionary which contain 10,000 words of length 8 each (all created using random combination of 16 NeuKlingon alphabets). Given this setup, please answer the following questions

(you need to show your detailed calculation)

5.1. Calculate the guess entropy of this password for a brute force attacker without any background knowledge about the dictionary (guess entropy = $\log_2$ (number of guesses))

5.2. Calculate the guess entropy of this password for a brute force attacker who has access to the full dictionary.

5.3. Calculate the *expected* guess entropy of this password for an attacker who has access to a random subset of 1000 words from the dictionary (hint: you need to use the *expected number of guesses*).

5.4. Now, assume the 4 words are chosen not at random---the frequency of picking words from the given dictionary is $f(w) = \frac{10000}{(w+3)^2}$ where w is the order in which a word appears in the dictionary. Calculate the *expected* guess entropy of a password for an attacker who has access to full 10,000-word dictionary and know this fact.

Question 6 | 2 x 6 = 12 marks

Please answer the following questions (in no more than 5 sentences each).

6.1. In "CCCC: Corralling Cookies into Categories with CookieMonster" by Hu et al. the mentioned encountering the OOV (out of vocabulary) problem? What is the OOV problem described in the context of the paper? How did they solve the problem?

6.2. In "Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing" paper Weinshel et al. mentioned that "Over 90% of participants were surprised by something presented in Longitudinal:Interests". Argue for or against this statement "Based on the results reported in this paper majority of users do not realize what topics the trackers can infer about their interests over time".

6.3. Define and describe (1 line each) any four principle of SPRUCE guidance on how to create effective security warnings and notices for end users

6.4. In "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research ", the Beneficence principle reflects the concept of appropriately balancing probable harm and likelihood of enhanced welfare resulting from the research. Explain what would you do to ensure beneficence in your research study design and why.

6.5. In "Rethinking Connection Security Indicator" paper Felt et al. first evaluated the "lock", "circle" and triangle. However, then they added an "exclamation" mark in the circle icon before deployment. What is the rationale of doing so?

6.6. Imagine you want to add an alt-text for the images in IIT Kgp website and you recruited Arun for this task. He added very detailed alt-text to describe the significance of each image. E.g., for IIT Kgp logo, Arun added "The official emblem of the first IIT in the nation, created in 1951, signifying the pursuit of knowledge which is at the heart of this institution". Is this a good or bad idea? Why?

Question 7 | 4 x 1 = 4 marks

Please answer the following questions. All oranges XD

7.1. A researcher is looking at the effect of eating oranges on the ability to solve a puzzle. There were 50 participants. The participants ate 3 ~~oranges~~, then solved the puzzle. The following day, the same participants came back, ate no bananas and then solved the same puzzle. We time how long it took them to solve the puzzle each time. How is the experiment best summarized?

A) Between-subjects design. Independent variable is whether oranges are eaten. Dependent variable is the time to solve the puzzle
B) Within-subjects design. Independent variable is whether oranges are eaten. Dependent variable is the time to solve the puzzle
C) Between-subjects design. Independent variable is the time to solve the puzzle. Dependent variable is whether oranges are eaten
D) Within-subjects design. Independent variable is the time to solve the puzzle. Dependent variable is whether oranges are eaten

7.2. Arun recruits some participants with iOS or Android phones running the latest version of each operating system. He runs security software on each phone and counts the number of security problems found. What statistical test is most appropriate for studying whether iOS or Android users have more security problems, on average? Choose all that apply.

A) Logistic regression
B) t-test/ANOVA
C) Pearson's Correlation
D) Chi-squared test

7.3. What is a Chi-Square test? Choose all that apply.

A) A significance test used to 4nalyse quantitative data
B) A significance test used to 4nalyse categorical data
C) A significance test used to 4nalyse quantitative and categorical data
D) A significance test used to 4nalyse parametric data

7.4. When would you use ANOVA instead of a t-test? Choose all that apply.

A) ANOVA should be used instead of a t-test for studies that have more than two conditions
B) ANOVA should be used instead of a t-test for comparing the means of multiple groups
C) ANOVA should be used instead of a t-test for between-subjects experiments involving 2 conditions
D) ANOVA should be used instead of a t-test for within-subjects experiments involving 2 conditions

---

Question 8 | 4 marks

What is your exact unique individual contribution (i.e., the tasks that *you* did) in your course project. Please describe in less than 5 sentences (preferably bullet points)

END OF QUESTION PAPER