Assignment 2: Personnel and Physical Security, Basic Cryptography
Due 6 February 11:59pm in Gradescope.
If using late days, enter "Using late days 2-4", or as appropriate.

1 Personnel and Physical Security Identification and Mitigation: ShopRite Data Security Incident

Please read the article:
`https://www.databreaches.net/millville-shoprite-experiences-data-security-incident/`

1. Identify one personnel or physical security vulnerability that was exploited as part of this incident (a few words, use terminology from the lectures.)j
2. Give a brief (1-2 paragraph) explanation as to how you could mitigate the security vulnerability you identified.

2 Personnel and Physical Security Identification and Mitigation: Credit Card Attacks

Please read the article
`https://www.theregister.co.uk/2010/10/27/credit_card_flash_attacks/`

1. Identify one personnel or physical security vulnerability that was exploited as part of this incident (a few words, use terminology from the lectures.)
2. Give a brief (1-2 paragraph) explanation as to how you could mitigate the security vulnerability you identified.

3 Personnel Security

In Questions 1 and 2, the URLs are not "hyperlinks", but just text (although some browsers recognize the text as a URL and allow you to click them - under Adobe Reader it is not clickable.) This is inconvenient - you have to cut/paste or retype rather than just clicking on the link.

From a personnel security point of view, why might we have chosen not to make this a hyperlink?

4 Training

When you originally signed up for a CS account, and likely at several other points in your Purdue career, some security awareness training was provided. Name or briefly describe a security awareness training activity you have experienced at Purdue. If you can't think of one, briefly explain why you can't, even though some have occurred.

5 Physical/Personnel Security Issues

For this question, you are asked to identify personnel and physical security vulnerabilities that arise in computer science labs, specifically LWSN B158. Complete the following table by identifying and briefly describing vulnerabilities to fill each of the six slots in the following table:

	Personnel	Physical
Confidentiality		
Integrity		
Availability		

While we do not ask you to describe how to mitigate the vulnerability, you should consider 1) would exploiting the vulnerability likely violate the security expectations of an educational lab, and 2) is it possible to mitigate this in a way that doesn't significantly reduce confidentiality, integrity, or availability (i.e., make the lab unusable.)

6 Crypto: Sample RSA Encryption

Consider a toy RSA example where: $p = 53$, $q = 79$, and $e = 5$
Find the ciphertext using RSA encryption for plaintext $P = 42$. Show all the steps you took to get to the final ciphertext.
(Reminder: Python makes an excellent calculator for large numbers!)

7 Crypto: Sample RSA 2

Using the same p, q, and e values from above, try to encrypt the plaintext $P = 0$.
Why is this an issue, and how is it typically dealt with in practice?

8 Crypto: Bad encryption mode

Assume some encryption scheme always encrypts the same plaintext into the exact same ciphertext when using the same key.

1. How does this leak information?
2. What could you do to solve this?

9 Crypto: Diffusion

Diffusion states that if we change a single bit of the plaintext, then every bit of the ciphertext should change with probability 0.5. Assume we are using a cipher that has poor diffusion: changing a bit in the plaintext only changes a few neighboring bits in the ciphertext. Explain how this could leak information under a chosen plaintext attack.