EECE 412, Fall 2009

Final Examination

Your Family name: ______________________________

Your Given name: ______________________________

Your student ID: ______________________________

Name of your left neighbor: ______________________

Name of your right neighbor: ______________________

#	Points	Out of
1		1
2		2
3		3
4		8
5		3
6		6
7		1
8		3
9		10
10		27
TOTAL		64

Attention: If to answer any of the following questions, you need to make additional assumptions, do so but specify these assumptions explicitly by writing "Additional assumptions: …"

1. "This final exam should not be accessible for this course students before the examination." Which one of the following properties pertaining to the final exam is the above statement about? (Check one most appropriate)

[ ] accountability
[ ] assurance
[ ] confidentiality
[ ] availability
[ ] integrity

2. Under certain circumstances, which of the following methods could encrypt identical plaintext to produce identical cyphertext? (pick one)

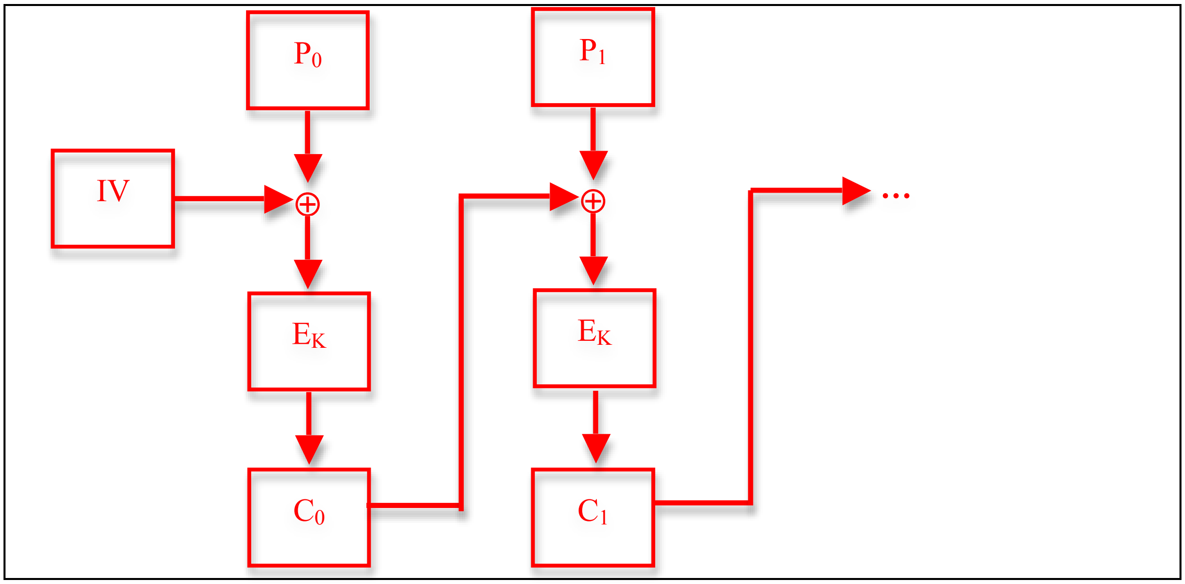
A. Caesar's Cipher
B. Vigenere's Cipher
C. One Time Pad
D. A and B from the above
E. B and C from above
F. A, B, and C from above

Answer: _____

3. Explain your answer to the previous problem:

4. Suppose that we use a mode of operation defined by the following rule:
$C_0 = E(IV \oplus P_0 , K), C_i = E(C_{i-1} \oplus P_i, K)$

(2 points) Draw this mode's diagram, similar to the ones Kosta used for illustrating modes of operation in class.



(2 points) What is the corresponding decryption rule?

$P_0 = IV \oplus D (C_0 , K), P_i = C_{i-1} \oplus E(C_i, K)$

(4 points) Explain security disadvantages of this mode, compared to CBC mode.

There are no any disadvantages because this mode of operation is exactly CBC.

5. In a digital signature scheme based on public-key cryptography, we compute the message digest first and then encrypt the result using the sender's private key: S = E(H(M), K). What if the process were reversed: S = H(E(M, K))?
Would it yield the same type of integrity protection? Explain why or why not. (Assume that the hash function and the encryption algorithm are strong.)

If the process were reversed, the receiver would not be able to verify the signature, because the verification requires encrypting message M with the sender's private key.

6. You are hired to lead the design and development of a security plug-in, an implementation of the reference monitor concept for the Web portal, for HSBC financial group. Since your team members have little experience with designing security mechanisms, you first need to explain them the three required properties of a reference monitor and why these properties are critical. Write down these three required properties, why they are important, and the principles of designing secure systems that these properties support/follow.

7. Give 1-2 examples that illustrate the difference between access control and authentication. Explain your examples.

Login in to a computer by providing user name and password is authentication.

Preventing an unauthorized user, who has logged into the computer, from reading a file is access control.

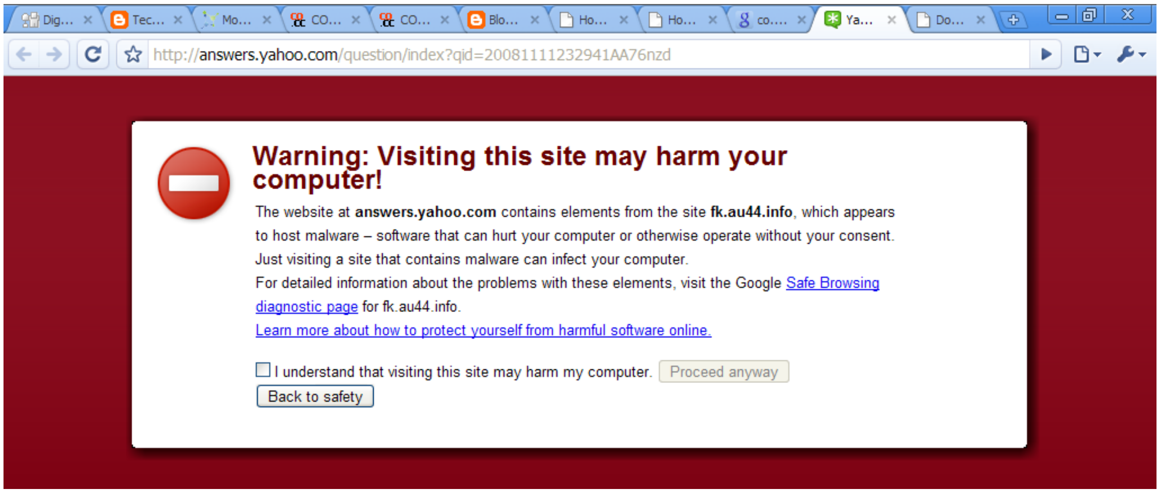
8. You are a consultant to the Ministry of National Defence (MND). The ministry is planning to update their physical security system, which currently uses two factors: 1) badge with person's name, picture, and, magnetic strip with the hash value of the 4-digit PIN, and 2) typing in a PIN. They want to keep the authentication system as it is, but increase the strength of the second factor, the PIN. Yes, in military, they can force employees to use random passwords or PINs.

You are asked to evaluate the following two alternatives and offer your opinion which option should be chosen by the MND:
1) upgrading to 6-digit random PINs, or
2) preserving the length of 4 characters but switching to letter-based password randomly chosen using 26-caharacter English alphabet.

Provide below your recommendation and the rationale for it. Assume that the attacker's goal is to find only the PIN/password for a specific (stolen) badge.

> The search space of 6-digit PINs is 10**6, which is 1,000,000. The space of 4-letter password is 26**4 = 456,976, which is a smaller search space than in the case of 6-digit random PINs. So, the 6-digit random PINs are better and should be recommended.

9. In the class on Usable Security, we discussed Cranor's Human in the Loop Framework developed to assess the usability of security warnings. This is the warning message from Google Chrome that will appear if the browser detects a site suspected of hosting malware. To get full points, make sure you are specific.


Dig...
Tec...
Mo...
CO...
CO...
Blo...
Ho...
Ho...
co....
Ya...
Do...
http://answers.yahoo.com/question/index?qid=20081111232941AA76nzd

Warning: Visiting this site may harm your computer!

The website at **answers.yahoo.com** contains elements from the site **fk.au44.info**, which appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that contains malware can infect your computer.

For detailed information about the problems with these elements, visit the Google Safe Browsing diagnostic page for fk.au44.info.

Learn more about how to protect yourself from harmful software online.

□ I understand that visiting this site may harm my computer. Proceed anyway

Back to safety

1. (2 points) Discuss how effective you believe the warning will be in terms of the attention switch aspect of communication delivery. Specify which elements of the warning help/hinder the attention switch.

Active warning so the user is forced to notice it. Other components include the icons, colour, etc. But the active warning is the big one.

2. (2 points) Discuss how effective you believe the warning will be in terms of the attention maintenance aspect of communication delivery. Specify which elements of the warning help/hinder attention maintenance.

The active warning also plays a role here. Forcing the user to check the box acknowledging the risk should help ensure that the user maintains attention long enough to process the warning (no easy click on the default left button – the default is to not proceed).

3. (2 points) Discuss whether the language used in the warning is understandable by a user such as yourself (ECE student, completed 412) and whether it helps with comprehension of the potential harm of proceeding. Does the warning contain enough information for you to decide whether or not to proceed?

Some reflection about appropriateness of terminology (e.g., definition of malware) and the ability of the user to comprehend the nature of the harm. When discussing whether or not to proceed, reflecting on security as a secondary task would be a bonus.

4. (2 points) Describe if and how your answer to Question 3 might change if the warning was viewed instead by someone with little technical or security knowledge?

Some acknowledgement that users with less technical/security knowledge might have a more difficult time understanding the concept of malware, that websites can contain elements from other websites, what an infected computer is, etc.

5. (2 points) Recently, there has been online discussion about the number of false positive identifications of malicious sites that trigger this warning. If a user is familiar with the high false positive rate, how will it affect the usability of this warning?

Discussion of affects of habituation – if a user thinks that he has seen it before and it was ok, or that this usually means that there isn't a problem, then he will be more likely to quickly click through without looking at the details of the specific problem in the warning.

10. The handout contains a reproduction of Chrome OS security overview.

a. **(7 points)** For each principle for designing secure systems, **put a checkmark** in the following table for those aspects of Chrome OS that **enable** or **follow** this principle.

Attention: The total number of points for this question will be determine using the following formula: $R - W$, where R is the number of right checkmarks and W is the number of wrong checkmarks.

	OS hardening	Making the browser more modular	Web app security	Phishing, XSS, and other web vulnerabilities	Secure autoupdate	Verified boot	Rendering pwned devices useless	Mitigating device theft	Data protection	Account management	Biometrics, smart cards, and Bluetooth	Login	CAPTCHAs	Auto-login	Single signon
Least Privilege															
Fail-Safe Defaults															
Economy of Mechanism															
Complete Mediation															
Open Design															
Separation of Privilege															
Least Common Mechanism															
Psychological Acceptability															
Defense in depth															
Question assumptions															

b. **(10 points)** Write justification for the checkmarks in the above table.

c. **(10 points)** Explain which particular aspects of malware and corresponding protection and detection techniques are used in these new features.