

CS 461 / ECE 422 Information Assurance
HW #2 KEY
Due submitted to Compass by 3:00 p.m. Feb. 5

The questions below prefaced by T/F are true-false questions. For these you must select one or the other, but may clarify your answer with more text if you wish.

1. **T/F** Security concerns are separate from software engineering concerns, so that an efficient way to design and implement software is to get its functionality right first, and later add security mechanisms. FALSE
2. Describe the difference between a constraint, a requirement, and a control in a security policy. SECTION 8.3 in TEXT
A **requirement** is a functional or performance demand on a system to ensure a desired level of security. A **constraint** is an aspect of a security policy that directs the implementation of a requirement. A **control** is a means of removing or reducing a vulnerability.
3. **T/F** Once a security policy has been established, one needs to review it and its effect on the system periodically but infrequently. ACTUALLY, EITHER T OR F is defensible. It must be periodic, frequency is in the eye of the beholder.
4. **T/F** The only people who are needed to develop a security policy are security experts and application experts. Since management doesn't understand either, it's only role is to adopt the plan developed by the experts. FALSE
5. Describe the difference between a business continuity plan, and an incident response plan. The former focuses on how to maintain the business in the event of lost capacity, the latter focuses on mitigating the actual incident.
6. **T/F** If one symmetric cryptographic method uses a longer key than another, it is more secure. FALSE—security depends on more than just key length.
7. **T/F** An important principle of symmetric cryptography is that keys and the data being encrypted are completely separate---in no way does a key depend on data values. FALSE-Streaming ciphers use keys that depend on data.
8. **T/F** It is critical for the functional operation of a Feistel network that the operation that combines the output of the f function with half the result from the previous stage be an XOR. In other words, no other function could replace the XOR, with no other changes to the Feistel network, and still have the property that decrypting is the same as encrypting, but with a reversed key schedule. FALSE. What is important is that the operation be its own inverse. While the XOR is the only bit function with this property, it is not the only function with that property

when we consider functions of more bits. Example $f(00) = 01$, $f(01) = 00$, $f(10) = 11$, $f(11) = 10$